THE CANTON NETWORK SERIES

PART 3 OF 5

# The Privacy Imperative for Stablecoin Payments

JULY 2025

Canton

Presented by The Tie

# Table of Contents

# Introduction

*In December 2024, three German marketing researchers inadvertently exposed the most critical threat facing every business using crypto or stablecoins for payments. Using only Python scripts and transparent payment and customer data from public blockchains, they decoded 22.7 million stablecoin transactions to expose share of wallet, how often people purchased items, average order prices, and peak sales times for eight direct-to-consumer companies—effectively turning public ledgers into open-source customer surveillance tools.*[1]

*This reveals a core contradiction at the heart of stablecoin infrastructure: the same networks revolutionizing the way money moves with instant, borderless payments also leave financial strategy and commercial behavior exposed to anyone with a block explorer. A generational breakthrough in payment efficiency is now facing a systemic privacy challenge—one that spans from individual salary leaks to enterprise-level treasury monitoring and threatens to undermine the next wave of growth and utility as global stablecoin volumes surge toward the $5 trillion mark.*

# Introduction (con’td)

*The Canton Network has introduced a fundamental shift in blockchain design, solving this challenge while retaining the interoperability across assets and applications that are so critical to unlocking the potential of tokenization. Unlike other public blockchains, where transactions are visible to all participants or are feebly attempted to be obfuscated through bolt-on privacy solutions, Canton implements privacy controls through programmable smart contracts and at the protocol level. Critically, this selective visibility model enables service providers to permission authorized parties—such as AML monitoring services like Elliptic and TRM—for real-time compliance oversight while maintaining privacy from unauthorized observers. This enables previously impossible financial workflows on-chain, such as private stablecoin transfers and settlement, B2B treasury operations, and regulatory-aligned asset tokenization to increase the utility of digital assets, for example as collateral - all without sacrificing auditability or composability.*

*Read more about how Canton and its tokenomics work on a technical level in Parts 1 and 2 of The Canton series here and here.*

*With over $4 trillion of assets tokenized or processed on the network today, including approximately $100 billion in daily UST repo, Canton demonstrates institutional-scale adoption at unprecedented levels. Tokenized cash providers that integrate with these asset flows—while delivering the privacy institutions require—represent a fundamental shift. Stablecoins evolve from an emerging institutional utility to the essential lubricant enabling the broader $500 trillion global capital markets to operate with 24/7 efficiency.*

[1] Source: https://www.researchgate.net/publication/387041111_Decoding_blockchain_data_for_research_in_marketing_New_insights_through_an_analysis_of_share_of_wallet

### Privacy Matters for Retail Payments

Crypto workers routinely face impossible choices when receiving stablecoin salaries. Spend directly from their salary wallet and expose their income to landlords, employers, and competitors—or route funds through centralized exchanges in complex multi-step processes that defeat the purpose of using crypto.

Privacy workarounds reveal the fundamental flaw: users are forced to choose between financial efficiencies and the basic privacy that traditional payment systems already provide. Stablecoins on public chains have the same problem Venmo used to have—where payments were public by default. A simple transaction to pay for medical treatment might seem harmless until something you didn't want known is exposed to an employer, an insurance firm, or a partner. Without privacy controls, that payment transaction becomes a lasting digital fingerprint—publicly accessible, tied to your wallet, and traceable forever.

### Free Insights for your Competitors

E-commerce businesses accepting stablecoin payments inadvertently provide competitors with free market research. Transaction timing patterns reveal peak sales periods. Payment clustering exposes customer acquisition strategies. Geographic analysis shows market expansion priorities. What traditionally required expensive corporate intelligence gathering now sits one blockchain explorer search away, easily decoded by a motivated competitor.

### Workplace Transparency Problems

Startups paying remote teams in stablecoins face the "salary visibility problem"—employees can see each other's compensation on-chain, creating workplace tensions that traditional payroll systems never expose. Companies must either have uniform and transparent salary policies or accept team morale issues, forcing many back to legacy payment rails despite their inefficiencies.

## Targeted Attacks Through On-Chain Intelligence

The February 2025 Bybit hack—resulting in $1.5 billion stolen, the largest crypto theft in history—demonstrates how transparent blockchain data can enable sophisticated targeted attacks. North Korea’s Lazarus Group used on-chain behavior analysis to understand Bybit’s internal transaction processes, timing patterns, and operational procedures. Fully transparent blockchains make transaction details (e.g., wallet addresses, amounts, and timestamps) publicly accessible via explorers, enabling attackers to analyze and identify high-value wallets, routine transfer schedules, or multisig operations.

The attackers specifically targeted Bybit’s Ethereum cold wallet operations, manipulating SafeWallet’s interface to disguise malicious transactions as routine transfers from cold to warm wallets—a pattern they had observed through months of on-chain surveillance.

## All Eyes on Treasury

When Arkham Intelligence tracked down 87.5% of MicroStrategy’s Bitcoin holdings—totaling $54.5 billion—despite sophisticated privacy measures, they demonstrated how transparency defeats even security-conscious institutions. Corporate treasury operations are left with the option of sticking to traditional rails with multi-day settlement and high fees – with the strategic confidentiality they need – or gaining the benefits of using stablecoins but at the risk of exposing pricing, treasury strategy, or sensitive investment positions. For institutional operations looking to engage on-chain, this transparency is a non-starter.

## Privacy Unlocks Scale

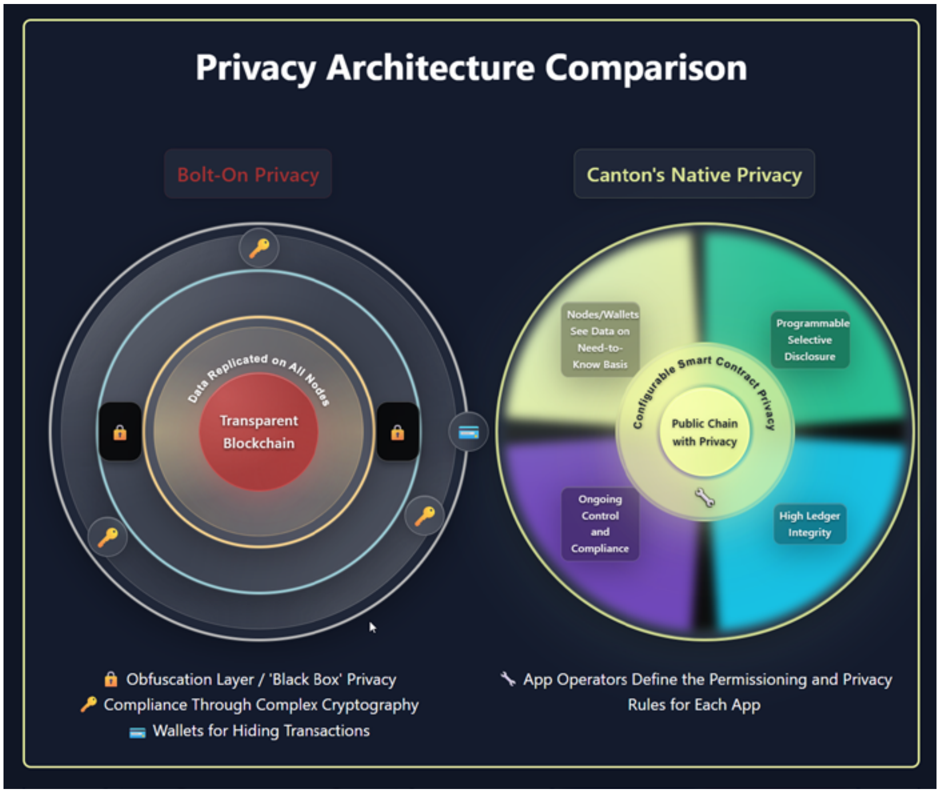
These privacy risks multiply exponentially with adoption. Imagine how this looks when you extrapolate the challenge to the trillions of dollars of daily flows across institutional capital markets. At current growth rates approaching $5 trillion in stablecoin volume, we're not discussing future problems—we're living the breakdown of business confidentiality in real-time. Every on-chain payment can violate individual privacy, create exploitable competitive intelligence, and disrupt business operations. From individual salary exposure to the movement of global collateral across today's crypto or traditional capital markets.

An entire industry has emerged for bolt-on obfuscation and confidentiality solutions for public blockchains. In 2025, there is news almost every week about an L1 or wallet provider acquiring or launching new technology workarounds, or entering partnerships to try to address the challenge. But the very nature of building complex obfuscation layers on top of chains that were designed for radical transparency remains a barrier to success. These approaches continue to hinder widespread institutional adoption and regulatory buy-in.

The Canton Network's recent surge in adoption underscores a growing institutional recognition: privacy must be built into the foundation—not patched on top—if stablecoins are to scale into the core infrastructure of global finance.

Today's proposed privacy solutions for public blockchains range from Zero-Knowledge Proofs to shielded wallets. While potentially useful for narrow use cases, these approaches introduce technical fragility and audit challenges that have been well documented. In contrast, Canton provides a configurable privacy model built directly into the protocol, enabling general-purpose, scalable privacy that is already proven to work at institutional scale.

## The Bolt-On Architecture Problem


Privacy Architecture Comparison
Bolt-On Privacy
Canton's Native Privacy
Data Replicated on All Nodes
Transparent Blockchain
Nodes/Wallets See Data on Need-to-Know Basis
Programmable Selective Disclosure
Configurable Smart Contract Privacy
Public Chain with Privacy
Ongoing Control and Compliance
High Ledger Integrity
🔒 Obfuscation Layer / 'Black Box' Privacy
🔑 Compliance Through Complex Cryptography
💳 Wallets for Hiding Transactions
🔧 App Operators Define the Permissioning and Privacy Rules for Each App

### Traditional Privacy Architecture (Fully Transparent Public Blockchains):

Because the first generation of public chains work by replicating all data across nodes, they must bolt-on complex solutions to engineer a level of obfuscation:

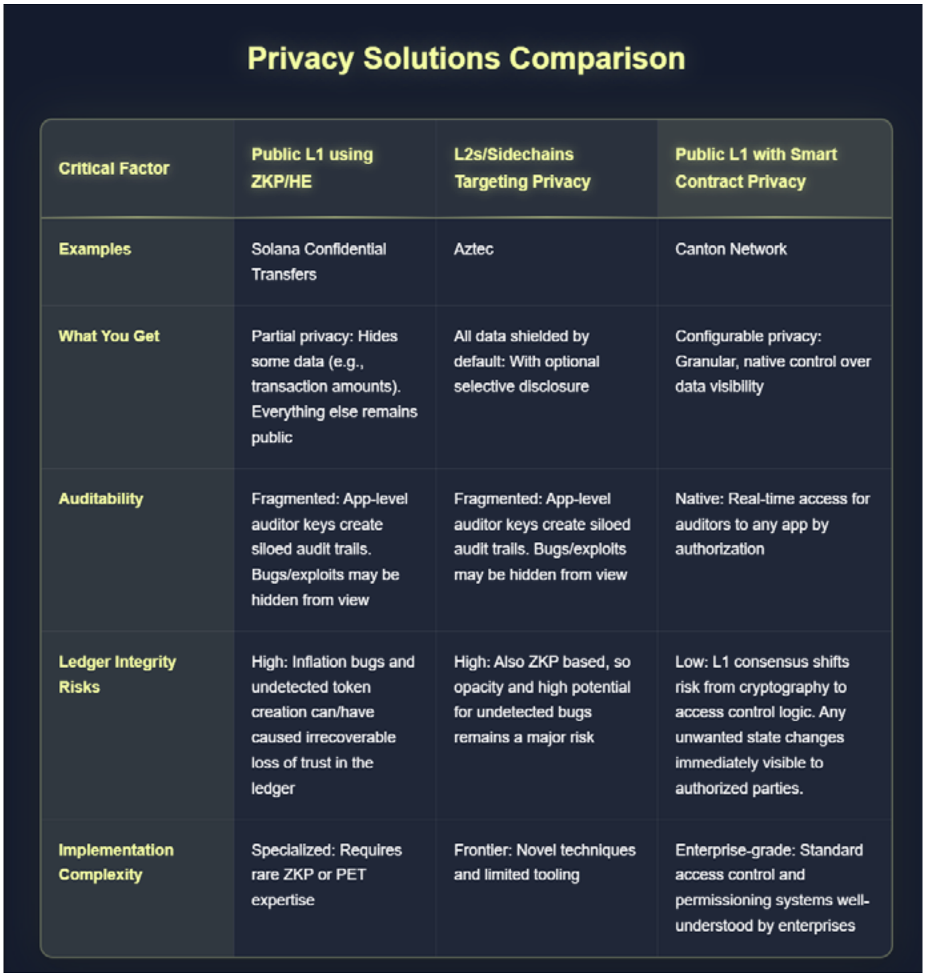
- **Core Layer**: Transparent base ledger (where everything is public)
- **Obfuscation Layer**: Add-ons like Zero Knowledge Proofs (ZKPs), Homomorphic Encryption (HE or FHE), mixers, and Layer 2 ZK-based solutions (note: ZK-rollups used in L2s are designed for scalability, not privacy)

- **Compliance Layer**: Auditor keys and selective disclosure tools (another bolt-on)
- **User Interface**: Complex “privacy” wallet integrations (aiming to hide transactions)

Each layer introduces failure points, operational complexity, and compatibility issues. Users must navigate bridge transactions, proof generation, specialized software, and regulatory compliance across multiple disconnected systems.

### Comparing Privacy Architectures

There is a fundamental divide between public infrastructure that must rely on Privacy Enhancing Technologies (PETs) such as ZKPs, and public infrastructure that employs smart contract level selective visibility by design. This highlights critical privacy considerations for any issuer, investor, or digital asset service provider involved in regulated financial workflows on-chain.



Privacy Solutions Comparison

| Critical Factor | Public L1 using ZKP/HE | L2s/Sidechains Targeting Privacy | Public L1 with Smart Contract Privacy |
|---|---|---|---|
| Examples | Solana Confidential Transfers | Aztec | Canton Network |
| What You Get | Partial privacy: Hides some data (e.g., transaction amounts). Everything else remains public | All data shielded by default: With optional selective disclosure | Configurable privacy: Granular, native control over data visibility |
| Auditability | Fragmented: App-level auditor keys create siloed audit trails. Bugs/exploits may be hidden from view | Fragmented: App-level auditor keys create siloed audit trails. Bugs/exploits may be hidden from view | Native: Real-time access for auditors to any app by authorization |
| Ledger Integrity Risks | High: Inflation bugs and undetected token creation can/have caused irrecoverable loss of trust in the ledger | High: Also ZKP based, so opacity and high potential for undetected bugs remains a major risk | Low: L1 consensus shifts risk from cryptography to access control logic. Any unwanted state changes immediately visible to authorized parties. |
| Implementation Complexity | Specialized: Requires rare ZKP or PET expertise | Frontier: Novel techniques and limited tooling | Enterprise-grade: Standard access control and permissioning systems well-understood by enterprises |

### Public L1 ZKP/PET Extensions: Partial Privacy Pitfalls

The limitations of using Zero-Knowledge Proofs (ZKPs) for scalable, general-purpose privacy are regularly highlighted by high-profile zero-day bugs. When vulnerabilities—like those enabling unlimited token minting—compromise the ledger, auditability is limited, leaving no reliable trail to verify the true state of the system. While ZKPs obscure transaction amounts, they still expose addresses, timestamps, and metadata—creating real risks and competitive intelligence leaks. On top of this, ZKPs and other PETs are computationally intensive, difficult to compose with, and prone to transaction bottlenecks—hindering smart contract integration.

### ZKP L2 Privacy Chains: Complexity and Composability Constraints

Privacy-focused L2 solutions like Aztec may find utility in niche anonymity applications, but they impose operational complexities that diminish institutional viability. Users face delayed 20-minute asset bridging, ZK proof generation for each operation, and liquidity isolation from the broader DeFi ecosystem. Trusted setup ceremonies for protocol upgrades present governance and operational risks that institutional risk management cannot accommodate.

Technical complexity and lack of mature standards limit native smart contract composability, restricting seamless transaction flows and value transfer across applications.

### Why Bolt-On Privacy Breaks Down at Scale

**Ledger Integrity Vulnerabilities**: Many ZKP systems require trusted setup ceremonies and complex cryptographic circuits that can harbor inflation bugs – enabling undetected token creation that appears valid to all participants. Historic vulnerabilities in various ZKP implementations demonstrate existential risks that a public network with smart contract-level privacy, by design, avoids entirely.

**Auditability Limitations**: ZKP-based privacy creates regulatory blind spots where institutions cannot provide the general purpose selective disclosure required for compliance. As Digital Asset's SEC submission notes: "ZKPs, as implemented today, provide only a limited form of privacy—they only shield data and do not offer the need-to-know transaction-level privacy necessary for regulated financial markets."

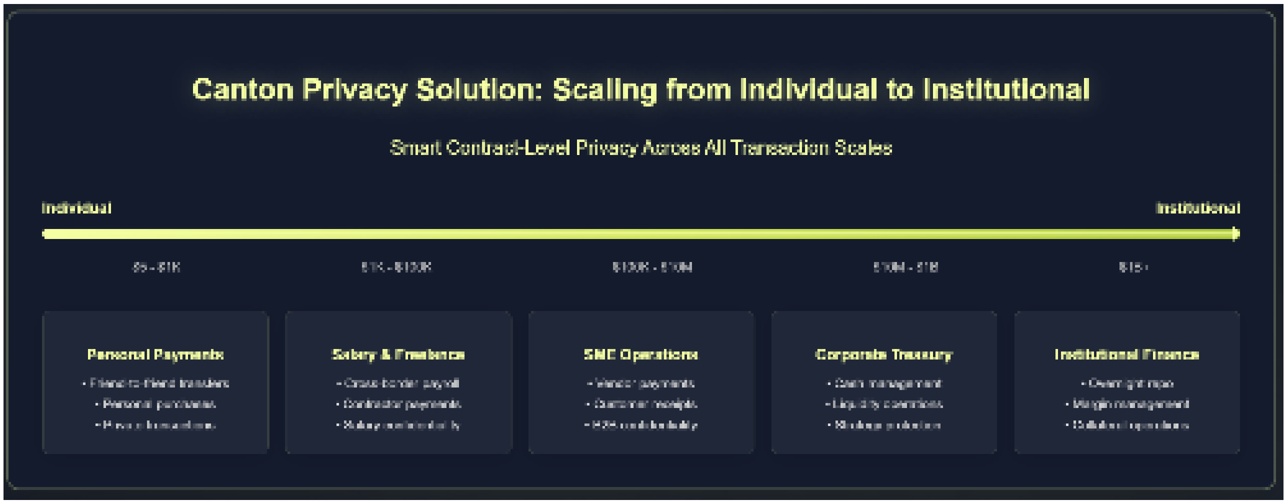
**Liquidity Fragmentation**: ZKP L2 implementations fragment liquidity across separate shielded pools, cutting participants off from broader network liquidity and creating operational inefficiencies for institutional users managing positions across multiple markets.

### The Centralization Irony

Other common "privacy" solutions involve using centralized exchanges as mixing services. This defeats DeFi's purpose while adding KYC requirements, freeze risks, and jurisdiction limitations, revealing the current inadequacy of such privacy tools. Even on-chain solutions like Tornado Cash have been famously targeted by OFAC sanctions via institutional blacklisting and subsequently trolled by poisoning celebrity wallets with thousands of dollars worth of Tornado Cash transfers.

Canton Network addresses these core limitations with a fundamentally different architectural approach.

### Canton: Configurable Privacy that Works



### Confidential Treasury and Vendor Payment Use Cases

Canton Network eliminates the "Venmo problem" for organizations and financial institutions—the permanent visibility that makes transparent blockchains unsuitable for business-grade payments:

- **Payroll Privacy**: Without such Layer 1 privacy, employees can see each other's compensation, creating internal conflicts and competitive disadvantages. Stablecoins that are deployed on Canton enable instant cross-border payroll, but with granular privacy.

- **Vendor Payment Privacy**: Transparent blockchains leak price-sensitive contract data, revealing negotiated rates and business relationships. On-chain payments made with tokenized cash on Canton protect commercial terms between counterparties.

- **Treasury Operations**: Without privacy, on-chain treasury and cash management activities expose cash flows and capital tables to competitors. Canton enables cross-border working capital and liquidity optimization with privacy, and the 24/7 convertibility of digital assets and stablecoins - not to mention the potential of Canton Coin rewards as an added incentive for firms to perform transactions on the network.

Bitwave's implementation demonstrates how enterprises can conduct privacy-preserving B2B stablecoin payments, keeping transaction amounts and counterparties confidential while preserving auditability for authorized regulators. Unlike today's fully transparent stablecoin infrastructure or bolt-on privacy workarounds, Bitwave supports end-to-end invoice payments with built-in SOC-compliant reporting and direct ERP integrations with systems like NetSuite and QuickBooks.

Stablecoin issuer Brale is also live on Canton and rapidly onboarding treasury teams to take advantage of confidential payments on Canton.

### Crypto Collateral and Margin Management Use Cases

Canton's privacy architecture transforms collateral management across traditional and crypto markets:

- **Safe Exchange Collateral**: Without Layer 1 privacy, transparent collateral flows invite front-running and push trades OTC. Canton enables private, composable collateral posting—combining tokenized yield-bearing treasuries for initial margin (IM) and stablecoins for variation margin (VM)—giving participants confidence they're on the right side of the trade.

- **Bilateral Derivatives Margining**: Transparent blockchains expose collateral movements, forcing overcollateralization and potentially missing yield opportunities. Canton enables bilateral margin management with privacy, allowing institutions to optimize capital, reduce tri-party costs, and earn additional yield.

Flowdesk, QCP, and other leading market makers are leveraging bilateral margin calls with privacy protections on Canton, not possible on transparent blockchains, where public margin contracts invite predatory trading from participants monitoring on-chain activity.

### 24/7 Capital Markets and On-chain Financing Use Cases

If the privacy that firms need is a given, then the ultimate promise of on-chain capital markets at scale becomes a reality. Think about the potential of instant liquidity across traditional and crypto capital markets with high-utility tokenized assets such as US Treasuries, and instant convertibility with stablecoins for 24/7 financing and risk management on-chain.

- **Liquidity Limitations**: Even stablecoins today are pegged to traditional financial rails, for example, over the weekend. Traditional finance cut-offs constrain liquidity, forcing institutions to hold excess cash to cover liquidity gaps between yield-bearing assets and stablecoins.

- **Canton's Solution:** With the confidence of privacy at scale, major institutions are working with Canton today to connect the dots, unlocking the ability to create/redeem stablecoins 24/7, instantly convertible with tokenized treasuries. Canton's privacy features ensure financing transactions remain confidential, protecting sensitive information about liquidity needs and collateral positions that would be exposed on other public blockchains.

This momentum is evidenced with major issuers like Circle coming to Canton, other major stablecoin providers like Paxos (a validator on Canton), and digital market infrastructure players like Ubyx recognizing Canton's fit for institutional stablecoin operations.

The stablecoin market stands at an inflection point. As volumes approach $5 trillion and institutional adoption accelerates, the expectations for privacy, compliance, and composability are no longer optional—they're foundational.

The infrastructure decisions made today will define who scales, who stalls, and who secures trust in the next era of capital markets and payments. Canton is not just a privacy solution—it is a proven model for how blockchain infrastructure can work to meet the demands of real-world finance.

For **stablecoin providers**, the opportunity is clear: become the institutional-grade digital cash that seamlessly plugs into tokenized repo, FX, payments, and collateral flows—without compromising on privacy, auditability, or compliance.

For **fintechs and builders**, it's a chance to offer next-generation financial services—wallets, payments, lending, or banking apps—that respect user confidentiality by default, while remaining fully composable with institutional financial flows. It's about unlocking new categories of on-chain finance—from confidential payroll and B2B payments to margin management and automated liquidity facilities—with privacy.

And for **asset issuers**, the path forward is infrastructure that not only supports high-utility tokenized real-world assets but ensures those assets can move and convert securely, privately, and at scale.

The question isn't whether blockchain infrastructure will support private financial workflows. It's already here. It's whether the industry will choose foundational privacy now, or pay the cost of retrofitting it later.

## DISCLOSURE AND FURTHER INFORMATION

This report is for informational purposes only and is not investment or trading advice. The views and opinions expressed in this report are exclusively those of the author, and do not necessarily reflect the views or positions of The Tie Inc. The author may be holding the cryptocurrencies or using the strategies mentioned in this report. You are fully responsible for any decisions you make; the Tie Inc. is not liable for any loss or damage caused by reliance on information provided. For investment advice, please consult a registered investment advisor. The Tie Inc. provides services to Digital Asset (US) Corp. In addition, The Tie Inc. operates as a founding super validator of the Canton Network and as such is eligible to mint and hold Canton Coin rewards based on the utility it provides to the Canton Network and its participants.

For questions about this paper or more information on the Canton Network, please contact research@thetie.io.

The Tie

The Tie Terminal™ is the leading information platform for institutions in digital assets. With its unmatched breadth and depth of proprietary data, our platform powers a consolidated workflow, giving professionals all the information they need to stay on top of the crypto market, and make more educated investment decisions.